REMARKS

In the July 3, 2003 Office Action, the Examiner rejected claims 1-14 under 35 U.S.C. § 102(b) as being anticipated by *Alanara et al.*, U.S. Patent No. 5,594,797. Taking care not to add new matter, Applicants have amended claims 1, 8, and 14 to point out aspects of the present invention and claims 3, 6, 10, and 13 to correct errors of a grammatical or clerical nature. Applicants submit that claims 1-14 are allowable over *Alanara et al.*

To anticipate a claim, the reference must teach every element of the claim. M.P.E.P. § 2131.01 (8th ed. 2001, revised February 2003). *Alanara et al.* does not disclose each and every element recited in the claims, so the rejections under 35 U.S.C. § 102(b) should be reconsidered and withdrawn.

For example, amended claim 1 recites, among other things, key conversions that output extended keys for direct use of encrypting plain text to cipher text or decrypting cipher text to plain text. *Alanara et al.* does not teach key conversions that output extended keys. Instead, *Alanara et al.* discloses a message encryptor with several transformation modules. Each transformation module receives a block of data and uses a key to transform the block of data. (*Alanara et al.*, col. 7, l. 48 - col. 8, l. 20; Fig. 3.) The transformation modules output transformed blocks of data, not extended keys for use in encrypting or decrypting text, as recited in claim 1.

Furthermore, *Alanara et al.* does not teach extended keys that result from key conversion functions. Instead, the keys used by the transformation modules of *Alanara et al.* are either received from a CPU or read from RAM. (*Alanara et al.*, col. 8, ll. 2-8.)

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

The reference does not disclose any key conversion functions that result in extended keys as recited in amended claim 1.

For at least these reasons, *Alanara et al.* does not disclose each and every element recited in claim 1. Therefore, Applicants respectfully request the reconsideration and withdrawal of the rejection of claim 1 under 35 U.S.C. § 102(b). Furthermore, claims 2-7 depend from claim 1. Because the reference does not recite every element of claim 1, it cannot recite every element of the claims that depend therefrom. Accordingly, Applicants request the reconsideration and withdrawal of the section 102(b) rejections of claims 2-7.

Amended claim 8 recites, among other things, a program comprising a key converting section that outputs extended keys for direct use of encrypting plain text to cipher text or decrypting cipher text to plain text. *Alanara et al.* does not teach such a structure. Instead, *Alanara et al.* discloses a message encryptor with several transformation modules. Each transformation module receives a block of data and uses a key to transform the block of data. (*Alanara et al.*, col. 7, l. 48 - col. 8, l. 20; Fig. 3.) The transformation modules output transformed blocks of data, not extended keys for use in encrypting or decrypting text, as recited in claim 8.

Furthermore, *Alanara et al.* does not teach extended keys that result from key conversion functions. Instead, the keys used by the transformation modules of *Alanara et al.* are either received from a CPU or read from RAM. (*Alanara et al.*, col. 8, ll. 2-8.) The reference does not disclose any key conversion functions that result in extended keys as recited in amended claim 8.

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

For at least these reasons, *Alanara et al.* does not disclose each and every element recited in claim 8. Therefore, Applicants respectfully request the reconsideration and withdrawal of the rejection of claim 8 under 35 U.S.C. § 102(b). Furthermore, claims 9-13 depend from claim 8. Because the reference does not recite every element of claim 8, it cannot recite every element of the claims that depend therefrom. Accordingly, Applicants request the reconsideration and withdrawal of the section 102(b) rejections of claims 9-13.

Finally, amended claim 14 recites, among other things, an apparatus comprising a key transformation section that outputs a second key and a third key by using an involution function. *Alanara et al.* does not teach a structure that outputs two keys by using an involution function. Instead, *Alanara et al.* discloses a message encryptor with several transformation modules. Each transformation module receives a block of data and uses a key to transform the block of data. (*Alanara et al.*, col. 7, l. 48 - col. 8, l. 20; Fig. 3.) The keys used by the transformation modules of *Alanara et al.* are either received from a CPU or read from RAM. (*Alanara et al.*, col. 8, ll. 2-8.) The reference does not disclose any involution functions that result in outputting two keys as recited in amended claim 14.

For at least these reasons, *Alanara et al.* does not disclose each and every element recited in claim 14. Therefore, Applicants respectfully request the reconsideration and withdrawal of the rejection of claim 14 under 35 U.S.C. § 102(b).

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

In view of the foregoing amendments and remarks, Applicant respectfully requests reconsideration and reexamination of this application and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.

Dated: December 3, 2003

By: William J. Brogan, Reg# 43,515
for Richard V. Burgujian
Reg. No. 31,744

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com